B. AMENDMENTS TO THE SPECIFICATION

Please amend the paragraphs of the specification as follows:

[0019] While credit card accounts are easy to commit fraud with because only a card number and expiration date are needed, other types of accounts may also be accessed by unauthorized persons. For example, an individual may establish a stock account accessible via the Internet with a user name and password. The server providing the stock account does not typically provide any fraud protection other than not releasing a [[A]]"forgotten password"[[@]] unless certain personal information is provided.

[0129] In analyzing the two tagged VID examples received at the fraud protection service for a single VID of [[A]]"Jon Smith"[[@]], one purchase is made via a telephone transaction on a wireless device. The other purchase is made via an in-store purchase transaction. Advantageously, the fraud protection service analyzes the location of [[A]]"Jon Smith"[[@]] identified by a GPS location of a cell phone utilized by [[A]]"Jon Smith"[[@]] compared with the store address in the second transaction and determines whether there is time for the user to move from one location to another. Other context may also be compared to determine if either charge is suspicious.

[0142] In analyzing this account access in view of the recent account accesses for [[A]]"Jon Smith"[[@]] it may be determined that Jon Smith could not log onto the stock service from a cell phone in Dallas, TX only minutes after making a purchase in a store in Austin, TX. Other context, such as the stock being purchased for a charity when the user has never purchased stock for a charity. Another set of context may compare the other amounts spent in other accounts according to VID with the average spending according to VID.

[0174] In the example, a call is placed by [[A]]"Jane Smith"[[@]] to [[A]]"Art's Parts"[[@]]. As illustrated by the authenticated callee identity 61, the call is initially received by a call center for [[A]]"Art's Parts"[[@]] and then transferred to a representative [[A]]"Jon Doe"[[@]] answering calls on behalf of [[A]]"Art's Parts"[[@]].

[0175] An authenticated caller identity **60** includes a VID name and a VID ID. The VID name and VID ID are preferably retrieved in response to a voice authentication by [[A]]"Jane Smith"[[@]]. In particular, additional encrypted information, such as a digital signature may be included with an authenticated caller identity. Further, an authenticated identity may also indicate, for example, the device utilized to perform the authentication, the frequency of identity of authentication, and the number to tries to achieve identity authentication.

[0188] Filtered suspicious charges **72** include context information for the third entry to be transferred to the account provider and/or the caller for authorization of the charge. Preferably, fraud protection service **56** monitors account transactions and designates suspicious charges prior to the transfer of funds or access to a service. In particular, a level of suspicion is assigned according to suspicious factors. For example, the third entry has a suspicion level of [[A]]"9"[[@]] because the call origination location is not accessible for the VID according to the previous activity and the shipping address is not only not indicated in the VID billing addresses, but is a P.O. Box.

[0194] In the example, the account provider preferences designate for the context of the entry to be transferred where the level of suspicion is [[A]]"1-3"[[@]]. Next, where the level of suspicion is [[A]]"4-8"[[@]], additional caller authorization is required and the context is transferred to the account provider. Finally, where the level of suspicion is [[A]]"9-10"[[@]] a decoy order completion is returned and the account transaction is reported to the authorities and the context is transferred to the account provider.

[0195] For the current VID, the internet purchase from TTT Toys is processed by returning a decoy order and notifying authorities because the level of suspicion is [[A]]"9"[[@]]. However, the internet purchase from HHH Holiday Suppliers is just reported to the account provider at level [[A]]"1"[[@]]. [[A]]"Jane Smith"[[@]] is prompted via one of the preferred communication media to provide additional authentication for the long distance call to continue.

[0217] Next, block **156** illustrates assigning a suspicion level to the context entry from [[A]]"0"[[@]] to [[A]]"10"[[@]], where [[A]]"0"[[@]] indicates no suspicion and [[A]]"10"[[@]] indicates a definite fraudulent use. Block **158** depicts controlling a response to the suspicion level according to the affected service/account provider preferences. In addition, the VID may include response preferences, particularly where the VID owner is responsible for charges incurred, even in the event of fraud. In addition, block **160** illustrates controlling output of the call context and authorization requirements according to the VID communication medium preferences, and the process ends.